Wireless LAN Security Guidelines

State of Iowa
Department of Administrative Services
Information Technology Enterprise
Information Security Office

Revision 1.4
April 19, 2004

“Writing a book on wireless security is like writing a book on safe skydiving – if you want the safety and security, just don't do it.”

– Ben Rothke, from his review of Russell Vines book, ‘*Wireless Security Essentials: Defending Mobile Systems from Data Piracy’*

Table of Contents

1. Abstract

Wireless communication technologies have flooded the marketplace and users are demanding that they be allowed to roam untethered. It has proven difficult to restrict their use due to the ease with which they can be set up.

These guidelines are intended for use by state agencies, citizens of Iowa, and the general public to educate them about the risks involved with wireless technology and assist them in securing their wireless networks.

2. Distribution

This document is available to the general public from the DAS/ITE Information Security Office website (http://das.ite.iowa.gov/security/), or by requesting a copy from SecurityAwareness@iowa.gov.

This document will be reviewed every six months or when significant threats emerge or changes in wireless technology occur. **Please check the distribution sources to ensure that you have the most recent version of this document.**

Comments, questions, suggestions, and concerns about this document should be sent to SecurityAwareness@iowa.gov.

3. Wireless Technologies

802.11, also referred to as Wi-Fi, consists of a family of protocols for wirelessly implementing Ethernet. Wireless transceivers, called access points (AP), are installed as just another element on the LAN. Computing devices such as laptops, desktops, PDAs, and printers can contain a wireless LAN card in place of the usual network interface card. Once the device establishes a link with the AP, it behaves as any other network device; the only difference being the data spends part of its time traveling through the air rather than over a wire.

Three of the 802.11 specifications relate to transmission frequencies and data rates. These specifications include 802.11b, 802.11a, and 802.11g.

> **802.11b**: The IEEE approved both the 802.11a and 802.11b standards in September 1999, but 802.11b devices beat 802.11a to market by about two years. As a result, 802.11b is far more prevalent. Many enterprises use 802.11b, though some later deployments have started using 802.11a and 802.11g, and these standards have their advantages and disadvantages. 802.11b utilizes the 2.4GHz band and has a top transmission rate of 11 Mbps. It has three non-overlapping channels.
>
> **802.11a**: The 802.11a specification offers several advantages over 802.11b. It operates at 5GHz, which makes it less susceptible to interference. It also utilizes a different transmission method, orthogonal frequency division multiplexing (OFDM), which passes data simultaneously along multiple sub-channels. Doing this results in a higher potential throughput rate of 54Mbps. In addition, 802.11a has eight different non-overlapping channels to choose from, rather than just three. But there are tradeoffs. The biggest is: as radio waves increase in frequency, range decreases. This is part of the reason why AM radio stations, which operate at a lower frequency, have a greater transmission distance than FM stations. With both 802.11a and 802.11b, the signal strength drops off the farther the user is from the nearest AP. As the signal strength drops, so does the data transmission rate. The higher frequency 802.11a signal drops off much more quickly than the 802.11b, giving it a limited range. This means that it requires more APs than 802.11b to cover the same area.
>
> **802.11g**: The 802.11g specification is designed to address the shortcomings of both the earlier standards. It has the same high 54Mbps data rate of 802.11a but does this over the wider range provided by 802.11b. It operates on the 2.4GHz frequency and is fully backwards compatible with 802.11b. This means that, if someone has an 802.11g card on their laptop, they can authenticate to APs that are using either the 802.11b or 802.11g protocols. An 802.11g device logged onto an 802.11b AP will shift down to the 802.11b data rate, so there is no advantage to 802.11g unless both are operating with 802.11g. In addition, for an AP to operate at 802.11g rates, every device logged onto it must be operating in 802.11g. If there is even one device using 802.11b, all the others revert to the lower protocol. AP devices can be set up to restrict the type of connection (e.g., 802.11g only) even if they technically can handle more than one type.

So, which one? 802.11g will be more useful to some degree in homes and in businesses where you can control the environment and make sure it is all 802.11g. But for enterprise settings, 802.11a offers the high data rate and is less susceptible to interference. Also, within a crowded office setting, the shorter transmission distance and greater number of channels can both be advantages. When you have a large number of users in a small space, you want to be able to put more access points in the area without their signals overlapping. Most vendors offer wireless devices that operate on all three standards.

Other wireless considerations include OpenAir, HiperLAN, HiperLAN2, HomeRF and SWAP, and possibly Bluetooth, but the focus of this document is on 802.11 wireless LAN technologies. Further reading on the other technologies mentioned above can be found in section 9 of this document. A wireless LAN glossary can be found in section 6 of this document.

4. Risks

In wireless LAN environments we must deal with all of the security issues that surround wired networks in addition to the issues that are introduced by the application of wireless technology. The through-the-air broadcast nature of wireless technology makes it less secure than wired networks. The following items identify known risks and associated threats that are present when using wireless network technologies.

4.1. RF Emissions

Wireless traffic is transmitted through the air using RF signals. These signals have the ability to penetrate windows, doors, walls, and other physical barriers exposing them beyond the physical proximity of your home or office. Customized high-gain directional antennas allow eavesdropping from long distances. This makes WLANs susceptible to the following threats:

- **Eavesdropping** – Unauthorized parties can view all data being transmitted through the air. This can include information about the configuration of your network as well as all data carried in the traffic sent over the air. If this traffic is not encrypted or poorly encrypted it is available for perusal by anyone within range of your access point.

- **Traffic Analysis** – Encrypted and unencrypted traffic can be analyzed for usage patterns using statistical analysis techniques. This can indicate when two parties are communicating and allow correlation of those patterns with real world events. For example, increased communication between two nodes could indicate that an event is about to occur.

- **Network Mapping** – Not long after wireless technology went mainstream people began engaging in an activity that came to be known as war-driving, where they would drive around in their cars looking for open access points. As the activity evolved these points were marked using global positioning systems (GPS) as well as with a technique known as war-chalking. Eventually we began to see these locations published on websites for everyone to see.

4.2. Electromagnetic Interference (EMI)

EMI is the disruption of operation of a device that is in the vicinity of an electromagnetic field in the RF spectrum. Microwave ovens, cordless phones, baby monitors, and other WLAN technologies can cause interference with wireless networks. This interference can be utilized by an attacker or occur naturally from other devices located within the vicinity of the WLAN to cause the following threats:

- **Data Corruption** – Interference can affect the integrity of the data in transit.

- **Denial of Service** – A denial/degradation of service condition can develop if a continuous source of interference prevents an access point from transmitting or receiving data, making it unavailable to wireless stations.

4.3. Physical Access Control

Just like wired networks, if a client can send traffic to a device, that client can flood the pipe with enough traffic to prevent legitimate traffic from being received. This is compounded by the inability to physically restrict access to who can connect to an access point.

- **Denial of Service** – Even though a client may not be able to authenticate and gain access to the network, they still reserve the ability to send traffic to the access point and attempt a connection. These packets must be at least minimally processed by the

access point to in order for them to be discarded, therein creating a denial of service opportunity.

4.4. Evolving Technology

The IEEE originally approved the 802.11 standard in 1997 and a revised edition on March 18, 1999. Since its inception, the 802.11 standard has had several attempts at security architecture to address the risks specific to wireless technology.

- **Unproven Protocols** – Security protocols for wireless technology are still evolving and are relatively immature as can be demonstrated by the wealth of research papers published and tools to exploit the discovered vulnerabilities.

- **Faulty Software** – No software is immune from bugs, and even with proven protocols, an improper software implementation can create security vulnerabilities.

4.5. Rogue Access Points

Rogue access points are access points that are not installed by authorized personnel and have not been approved for use. These types of access points can be setup by employees or an attacker. The ease with which access points can be setup by even novice users makes the rogue access point a credible threat.

- **Circumventing security controls** – Having a rogue access point on your internal network usually means that it has been improperly configured and most likely bypasses security controls such as firewalls or other packet filtering devices giving attackers easy entry into your network.

- **Eavesdropping** – Access points managed by malicious users allow them to control all traffic passing through the access point.

4.6. Inexperienced Users

The most prevalent cause of security holes in wireless network stems from the lack of experienced users. As stated earlier the ease with which wireless technology can be installed and made to work is also one of the greatest causes of wireless security problems. This problem is much more prevalent in home use than government or corporate use, but it still exists. Hopefully this document will help guide these users in the right direction.

5. Considerations and Guidelines

The following are suggestions for implementing a wireless LAN as securely as possible. Wireless technologies, protocols, and standards are still emerging and evolving. **Please check the distribution sources in section 2 to make sure you have the most recent version of this document.**

5.1. Architecture

1. Wireless LAN's should be configured in infrastructure mode, as opposed to ad-hoc mode, to prevent peer-to-peer communication and allow greater control for monitoring usage.

2. Traffic from the wireless access point should not be allowed to travel unfiltered into the wired network. A firewall or other packet-filtering device should be placed between the access point and the wired network (See Figure 1 - Wireless LAN Architecture).

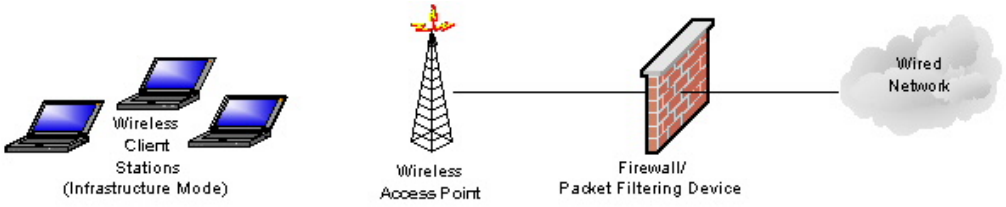

Figure 1 - Wireless LAN Architecture

3. Mission critical servers and other devices that are required to be available and provide reliable service should not be placed on the wireless network due to its high susceptibility to denial of service (DoS) attacks and disruption caused by RF interference, malicious or unintentional. Use of the wireless network should be limited to client workstations.

5.2. Physical Security

1. The wireless access point or base station should not be installed in an unprotected location where it can be exposed to theft, damage, or otherwise unauthorized access.

2. Efforts should be made to decrease the amount of RF leakage when designing your WLAN. Ensure that appropriate antennas are used and directed at the intended area of coverage; power and signals should not be boosted unnecessarily. An effective, but highly cost prohibitive option, is to install shielding in walls and windows to prevent leakage.

5.3. Registration

1. All wireless access points should be registered with a trusted registration authority. This registration gives network administrators the ability to check for access points within their vicinity to identify conflicts that may interfere with their wireless networks. This data has the additional benefit of being able to assist in identifying rogue access points.

5.4. Network Name

1. The network name (SSID) should be set to a name that does not easily identify the owner, purpose, or location of the base station. For example, instead of assigning an SSID of **IOWAPAYROLL** consider using something like **IBSP1** (**I**owa **B**ase **S**tation **P**ayroll **1**). These names would be useful to people who know the system, but not to outsiders.

2. The base station should not broadcast its network name (SSID). The client should be required to obtain this information from their network administrator.

5.5. Encryption and Authentication

1. Access points should take advantage of the MAC filtering capabilities found on most access points. Only connections from recognized MAC addresses should be accepted. *Please note: Most wireless network drivers allow the MAC address to be changed; this guideline should not be considered a stand-alone measure, but just another layer of a defense-in-depth strategy.*

2. A good rule of thumb is to treat wireless connections as you would an Internet connection, as an untrusted network. There are a large number of open and proprietary security solutions available for wireless networks. Most of these have had vulnerabilities or attacks performed against them. The most trusted form of security for WLANs involves requiring users to establish a VPN connection in order to access the wired network.

3. WEP is considered broken and ***should not*** be used. There have been several research papers written that address the insecurities of Wired Equivalent Privacy (WEP) security protocol [3,4,6,8,9].

4. LEAP is a Cisco proprietary protocol that is susceptible to brute-force dictionary attacks [2,10]. In response to this attack, Cisco released the EAP-Fast protocol that sends login credential through an encrypted tunnel. Users of LEAP should also consider the impact of using a proprietary technology.

5. 802.1X has been subjected to successful *man-in-the-middle* and *session-hijacking* attacks. [5]

6. Offline dictionary attacks have been performed against WPA when used with short pre-shared-keys [11]. If you use WPA with pre-shared keys be sure to select a key with 20 or more characters to mitigate the risk of this attack.

7. Currently, PEAP is the most accepted solution if you decide you are not going to require users to establish a VPN connection.

5.6. Event Logging

1. Access points should be configured to log data to a location where it can be reviewed for security violations.

2. Log data should contain enough information to accurately identify the event that occurred and correlate it with other systems.

3. Events to log include successful and failed access attempts, access point error and failures, reboots, etc.

5.7. Intrusion Detection

1. An intrusion detection system (IDS) should be used to detect both attacks and inappropriate use of the network.

2. In addition to watching for active attacks on the network, the IDS should watch for rogue access points, unencrypted traffic, and clients operating in ad-hoc mode.

5.8. Awareness

1. Users should be made aware that their data is traveling through the air and it is susceptible to interception.

2. Users should be made aware that the network is susceptible to disruption from a variety of environmental factors such as those mentioned in section 4.2.

6. Wi-Fi Glossary

802.11: Refers to a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

Access Point (AP): A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service to which a wireless user has access.

Ad-Hoc Mode: An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode also is referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required. We do not recommend using this method for wireless connectivity.

Base Station – *See Access Point*

Basic Service Set (BSS) – *See Infrastructure Mode*

Bluetooth: A short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. Products with Bluetooth technology must be qualified and pass interoperability testing by the Bluetooth special interest group prior to release. Bluetooth's founding members include Ericsson, IBM, Intel, Nokia and Toshiba.

Extended Service Set (ESS) – *See Infrastructure Mode*

Extensible Authentication Protocol (EAP): An extension to PPP, EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-Fast): Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks.

HomeRF: Home radio frequency. Designed specifically for wireless networks in homes, in contrast to 802.11, which was created for use in homes and businesses. HomeRF networks are designed to be more affordable to home users than other wireless technologies. Based on frequency hopping and using radio frequency waves for the transmission of voice and data, HomeRF has a range of up to 150 feet.

HiperLAN / HiperLAN2: High performance radio local area network. Developed by the European Telecommunications Standards Institute, HiperLAN is a set of WLAN communication standards used chiefly in European countries.

Independent Basic Service Set (IBSS) – *See Ad-Hoc Mode*

Infrastructure Mode: An 802.11 networking framework in which devices communicate with each other by first going through an access point (AP). In infrastructure mode, wireless AP devices can communicate with each other or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations, it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Lightweight Extensible Authentication Protocol (LEAP): This is a standard developed by Cisco. EAP-LEAP uses a username/password combination to transmit the identity to a RADIUS server for authentication.

Protected Extensible Authentication Protocol (PEAP): Pronounced, “peep,” this is a protocol developed jointly by Microsoft, RSA Security and Cisco for transmitting authentication data, including passwords, over 802.11 wireless networks. PEAP authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.

Radio Frequency (RF): Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

Robust Security Network (RSN) – A proposed IEEE security architecture for 802.11 that utilizes 802.1X.

Service Set Identifier (SSID): A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID also is referred to as a network name because, essentially, it is a name that identifies a wireless network.

Station (STA) – Any wireless device in an 802.11 network.

Temporal Key Integrity Protocol (TKIP) – Protocol used by WPA to improve the data encryption deficiencies of WEP.

Wireless Fidelity (WiFi): Used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, etc. The term is promulgated by the Wi-Fi Alliance. Any products tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a "Wi-Fi Certified" product should be able to use any brand of access point with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) will work with any other, even if not "Wi-Fi Certified." Formerly, the term

"Wi-Fi" was used only in place of the 2.4GHz 802.11b standard, but the alliance expanded the generic use of the term in an attempt to stop confusion about wireless LAN interoperability.

Wi-Fi Protected Access (WPA): A Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP, but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

Wired Equivalent Privacy (WEP): A security protocol for wireless local area networks defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

Wireless LAN (WLAN) – A LAN where devices connect to the network using wireless technology.

7. References

[1] J. Wright, “Detecting Wireless LAN MAC Address Spoofing”, January 21, 2003.

[2] J. Wright, “Weaknesses in LEAP Challenge/Response”, Defcon 2003.

[3] W. A. Arbaugh, N. Shankar, J. Wang, and K. Zhang, “Your 802.11 network has no clothes”, University of Maryland, Department of Computer Science, March 30, 2001.

[4] Stubblefield, Ioannidis, Rubin, “AT&T Labs Technical Report TD-4ZCPZZ”, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, August 21, 2002, Revision 2.

[5] A. Mishra, W. Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard”, University of Maryland, Department of Computer Science, February 6, 2002.

[6] S. Fluhrer, I. Mantin and A. Shamir, “Weakness in the Key Scheduling Algorithm of RC4”, Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[7] N.Borisov, I. Goldberg, D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”, Presented at the 7th Annual International Conference on Mobile Computing and Networking, July 19, 2001.

[8] W. A. Arbaugh, “An inductive chosen plaintext attack against WEP/WEP2”, IEEE Document 802.11-01/230, May 2001.

[9] J. R. Walker, “Unsafe at any key size; an analysis of the WEP encapsulation”, IEEE Document 802.11-00/362, Oct. 2000.

[10] Cisco Systems, “Dictionary Attack on Cisco LEAP Vulnerability”, Document ID 44281, http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml, August 3, 2003.

[11] R. Moskowitz, “Weakness in Passphrase Choice in WPA Interface”, http://wifinetnews.com/archives/002452.html, November 4, 2003.

8. Tools

AirSnort (http://airsnort.shmoo.com/)
AirSnort is a wireless LAN (WLAN) tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

Asleap (http://asleap.sourceforge.net/)
Asleap is a tool to recover passwords from a Cisco LEAP wireless network. This tool is released as a proof-of-concept to demonstrate a weakness in the LEAP protocol.

bsd-airtools (http://www.dachb0den.com/projects/bsd-airtools.html)
bsd-airtools is a package that provides a complete toolset for wireless 802.11b auditing. Namely, it currently contains a bsd-based WEP cracking application, called dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based AP detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned AP's and view statistics for each. It also includes a couple other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode.

Kismet (http://www.kismetwireless.net/)
Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

NetStumbler (http://www.netstumbler.com/)
NetStumbler is a Windows utility for 802.11b based wireless network auditing.

WEPCrack (http://wepcrack.sourceforge.net/)
WEPCrack is an open source tool for breaking 802.11 WEP secret keys. This tool is an implementation of the attack described by Fluhrer, Mantin, and Shamir in the paper "Weaknesses in the Key Scheduling Algorithm of RC4".

9. Additional Reading

SANS Institute 2003, “Security Guidelines for Wireless LAN Implementation”
http://www.sans.org/rr/papers/index.php?id=1233

HiperLAN2 Homepage, http://www.hiperlan2.com

Proxim Wireless Networks, http://www.proxim.com

Official Bluetooth Website, http://www.bluetooth.com

Wi-Fi Terminology Reference, http://wi-fiplanet.webopedia.com